

PATENT

HFC
Faw



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants: Sarvar PATEL et al.
Appl. No.: 10/786,454
Filing Date: February 26, 2004
Art Unit: 2439
Examiner: R. Tolentino
Title: METHOD OF GENERATING A CRYPTOSYNC
Atty. Dkt. No.: 29250-002013/us

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Mail Stop Appeal Brief

Date: March 5, 2012 (Monday)
(March 3 being a Saturday)

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

In response to the Examiner's Answer of January 3, 2012 and in accordance with the provisions of 37 C.F.R. § 41.41, Appellants submit the following Reply Brief.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

I. STATUS OF CLAIMS

Claims 1-24 are pending in the present application, with claims 1 and 24 being independent.

II. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Appellants seek the Board's review of the rejection of claim 5 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.¹

B. Appellants seek the Board's review of the rejection of claims 1, 4, 6, 7, 11, and 12 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication 2005/0086468 to Meandzija et al. ("Meandzija") in view of U.S. Patent Publication 2004/0078334 to Malcolm et al. ("Malcolm").

C. Appellants seek the Board's review of the rejection of claims 2 and 3 under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm in further view of U.S. Patent Publication 2005/0172116 to Burch et al. ("Burch").

D. Appellants seek the Board's review of the rejection of claim 5 under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm in further view of U.S. Patent Publication 2005/0177715 to Somin et al. ("Somin").

E. Appellants seek the Board's review of the rejection of claims 8-10 and 13-23 under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm in further view of U.S. Patent 6,980,658 to Rezaifar et al. ("Rezaifar").

¹ Appellants note the indication on page 12 of the Examiner's Answer that the rejection of claim 5 under 35 U.S.C. § 112, second paragraph has been withdrawn. Accordingly, Appellants present no further arguments with respect to this rejection.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

F. Appellants seek the Board's review of the rejection of claim 24 under 35 U.S.C. §103(a) as being unpatentable over Meandzija in view of Malcolm and Burch.

III. ARGUMENT

In addition to the arguments articulated in the Appeal Brief of November 3, 2011 (hereinafter, "the Appeal Brief"), Appellants would like to clarify the following points. However, it should be understood that any portion of the January 3, 2012 Examiner's Answer (hereinafter, "the Examiner's Answer") that is not specifically addressed herein is not a concession as to the propriety of that portion. Rather, the absence of a specific reply to such a portion is merely because clarification was not needed in view of the arguments already articulated in the Appeal Brief.

A. THE INTERPRETATION IN THE EXAMINER'S ANSWER OF THE TERM CRYPTOSYNC RECITED IN CLAIM 1 IS INCONSISTENT WITH APPELLANTS' SPECIFICATION

Appellants respectfully submit, during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification."² The broadest reasonable construction must be given "in light of the specification as it would be interpreted by one of ordinary skill in the art."³

The Examiner's Answer asserts that a cryptosync in the "broadest interpretation" is anything from a counter to an encryption key of a digital certificate

² *Phillips v. AWH Corp.*, 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005).

³ *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004).

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

or a number of other pieces of information.⁴ This assertion was not present in the June 3, 2011 Office Action (hereinafter, "the Office Action"). Further, Appellants respectfully submit the interpretation used in the Examiner's Answer is not the proper interpretation. To the contrary, as is discussed above, proper interpretation is the broadest *reasonable interpretation in light of the specification as it would be interpreted by one of ordinary skill in the art.*

Appellants' specification explains that a cryptosync is an element with a varying value. Appellants' specification further describes, as an example use of the cryptosync, input of the cryptosync into an encryption algorithm to generate a mask for use in encryption. The varying value of the cryptosync ensures that the result of encryption also varies, thus preventing replay attacks.⁵

Appellants respectfully submit that the Examiner has provided absolutely no support for the assertion that a person of ordinary skill in the art, in light of Appellants' specification, would determine the broadest reasonable interpretation of the recited term "cryptosync" to cover any piece of cryptographic information including an encryption key, a digital certificate or a number of other pieces of information as is asserted by the Examiner's Answer.

Further, Appellants respectfully submit a person of ordinary skill in the art, in light of at least the above-referenced portion of Appellants' specification, would understand the term cryptosync to denote an element that changes over time. Appellants respectfully submit this understanding is further demonstrated by one of the references of record, Rezaiifar.⁶

⁴ Examiner's Answer at p 12, l. 5-8.

⁵ Spec. at p. 2, l. 3-17.

⁶ Rezaiifar at column 4, lines 50-60 describes the variable nature of a cryptosync.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

Accordingly, Appellants respectfully submit the interpretation of the recited term cryptosync articulated in the Examiner's Answer is improper. Further, Appellants respectfully submit it is this improper interpretation which the Examiner's Answer uses as support for the assertion that digital certificates of Meandzija and Malcolm teach the first and second cryptosyncs recited in claim 1. Accordingly, Appellants respectfully submit the assertion that any of the session certificate of Meandzija, or the root or derived certificates of Malcolm teach either of the first and second cryptosyncs recited in claim 1 is incorrect, at least because digital certificates do not vary, which a person of ordinary skill in the art would require of a cryptosync. Specifically, Appellants respectfully submit the Examiner's Answer has provided no support for the assertion that a person of ordinary skill in the art would determine the broadest reasonable interpretation of the term "cryptosync", in light of Appellants' specification, to include a digital certificate. Accordingly, Appellants respectfully submit the "first cryptosync" and "second cryptosync" recited in claim 1 have not been identified in the applied art by the Office Action or the Examiner's Answer..

For at least the reasons discussed above, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that each of the limitations of claim 1 are taught or otherwise rendered obvious by the applied art as is required to support a rejection under §103.

B. THE EXAMINER'S ANSWER DOES NOT ACCOUNT FOR THE LACK OF A REASONING HAVING A RATIONAL UNDERPINNING SUPPORTING THE LEGAL CONCLUSION OF OBVIOUSNESS WITH RESPECT TO CLAIM 1.

In section VII(B)(3) of the Appeal Brief, Appellants argued that the Examiner had provided no reasoning having a rational underpinning supporting the legal conclusion of obvious with respect to claim 1, as is required to support an obviousness rejection according to *KSR*⁷. Specifically, on page 22 of the Appeal Brief, Appellants argued that benefits cited by the Office Action and discussed in paragraph [0028] of Malcolm were insufficient to motivate one of ordinary skill in the art to combine the teachings of Meandzija and Malcolm as the Office Action asserts, because the Office Action identified nothing in Malcolm attributing the benefits discussed in paragraph [0028] of Malcolm specifically to the use of a root certificate and a digital certificate derived therefrom as discussed in paragraph [0145] of Malcolm.

In response to the arguments above, page 15, line 6 to page 16, line 4 of the Examiner's Answer reference paragraph [0028] of Malcolm as evidence that combining the teachings of Meandzija and Malcolm would provide the advantage of having secure communications during a session. Appellants assume the Examiner's Answer is asserting that a person of ordinary skill in the art would be motivated to combine the teachings of Meandzija and Malcolm in order to provide secure communications during a session. However, the Examiner's Answer provides no support for this assertion. Specifically, as is admitted in lines 14-19 on page 15 of the Examiner's Answer, the system of Meandzija already provides secure communication and already

⁷ *KSR Int'l Co. v. Telefax Inc.*, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)

uses session certificates to do so. Accordingly, the Examiner's Answer does not explain why a person of ordinary skill in the art would be motivated to combine the teachings of Meandzija with those of Malcolm to achieve secure communications during a session, when Meandzija already teaches provision of secure communications during a session without the features of Malcolm.

Consequently, Appellants respectfully submit neither the Office Action nor the Examiner's Answer have articulated a reasoning having a rational underpinning supporting the legal conclusion of obviousness with respect to claim 1.

C. THE EXAMINER'S ANSWER DOES NOT ACCOUNT FOR THE FAILURE TO ESTABLISH A PRIMA FACIE CASE OF OBVIOUSNESS WITH RESPECT TO ANY OF CLAIMS 4, 6, 7, 11 AND 12.

Claim 4

Claim 4 recites "wherein the second cryptosync is used for verifying message integrity by at least one of the two devices". In the Appeal Brief, Appellants provided arguments explaining why paragraph [0007] of Meandzija failed to teach these limitations of claim 4. In response, the Examiner's Answer again references paragraph [0007] of Meandzija and asserts that Meandzija as modified by Malcolm teaches the above-referenced limitations of claim 4. Appellants respectfully disagree.

Specifically, the Examiner's Answer asserts the second cryptosync recited in claim 1 is taught by a root certificate disclosed by paragraph [0145] of Malcolm.⁸ The Examiner also provides a discussion on page 14 of the Examiner's Answer regarding

⁸ Examiner's Answer at p. 14, generally.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

root certificates and trees for which no citation is provided. Consequently, The Examiner's Answer has not established that the discussion on page 14 constitutes prior art which can be used to support a rejection of claim 14. Regardless, the Examiner has identified nothing in Malcolm, or any other cited art, teaching the root certificate of Malcolm being used, by at least one of two devices, to verify message integrity.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 4 as is required to support a rejection under §103.

Claim 6

Claim 6 recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync". On page 25 of the Appeal Brief at lines 12-22, Appellants argued that the above-referenced limitations of claim 6 were not taught by the mere disclosure of Malcolm regarding a certificate being derived from a root certificate, as the Office Action asserted.

In response, lines 7-12 of page 17 of the Examiner's Answer include an assertion that the meaning of the term "derive" is "to obtain from a source", and thus, a first digital certificate derived from a second digital certificate must have at least a portion of the second digital certificate. Appellants respectfully disagree.

Specifically, using the definition of derive provided by the Examiner's Answer, it is not necessary for a first object derived from a second object to include a portion of the second object. For example, cypher text can be derived from plain text by

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41
Atty. Dkt. No. 29250-002013/US
U.S. Appl. No. 10/786,454

inputting the plain text in an encryption algorithm. However, it is certainly not necessary for the cypher text to include any portion of the plain text. To the contrary, it is desirable for there to be no intelligible link between the cypher text and the plain text from which it is derived, at least not without the aid of a decryption algorithm. Accordingly, Appellants respectfully submit the assertion made by the Examiner's Answer that the definition of the term 'derived' requires the derived certificate of Malcolm to include at least a portion of the root certificate of Malcolm is false. The definition provided by the Examiner's Answer for the term "derived" requires only that the second certificate from which a first certificate is derived be a source, not that any portion of the second certificate is contained in the derived first certificate.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 6 as is required to support a rejection under §103.

Claim 7

Claim 7 recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence". On page 26 of the Appeal Brief at lines 1-12, Appellants argued that the above referenced limitation of claim 6 were not taught by the mere disclosure Malcolm regarding a certificate being derived from a root certificate.

In response, the portion of the Examiner's Answer at page 17, line 13 to page 18, line 8 appears to reference, again, the assertion made with respect to claim 6 that the meaning of the term derive is "to obtain from a source", and thus, a first digital

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41
Atty. Dkt. No. 29250-002013/US
U.S. Appl. No. 10/786,454

certificate derived from a second digital certificate must have at least a portion of the second digital certificate. Appellants respectfully disagree for the same reasons discussed above with reference to claim 6.

Further, Appellants note the discussion at lines 1-8 of page 18 of the Examiner's Answer regarding all digital certificates derived from the root certificate to have the same length. However, the Examiner provides no support for the assertions made in this discussion in the cited art or any other source.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 7 as is required to support a rejection under §103.

Claim 11

Claim 11 recites "wherein the deriving step derives a portion of the first cryptosync as the second cryptosync". On page 26 of the Appeal Brief at lines 15-24, Appellants argued that the above referenced limitations of claim 11 were not taught by the mere disclosure Malcolm regarding a certificate being derived from a root certificate, as the Office Action asserted.

In response, the Examiner's Answer provided the same arguments discussed above with respect to claim 6. Accordingly, Appellants respectfully disagree for the same reasons discussed above with reference to claim 6.

Further, Appellants note claim 11 requires a portion of the first cryptosync to be the whole second cryptosync, not merely a part of the second cryptosync. Accordingly, Appellants respectfully submit the broad, general discussion of a

certificate being derived from a root certificate provided in paragraph [0145] of Malcolm is clearly insufficient to teach the specific requirement that a portion of the first cryptosync be derived **as the second cryptosync**.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 11 as is required to support a rejection under §103.

Claim 12

Claim 12 recites "wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence". On page 27 of the Appeal Brief at lines 2-15, Appellants argued that the above referenced limitations of claim 12 were not taught by the mere disclosure Malcolm regarding a certificate being derived from a root certificate, as the Office Action asserted.

In response, the Examiner's Answer provided the same arguments discussed above with respect to claim 7. Accordingly, Appellants respectfully disagree for the same reason discussed above with reference to claim 7.

Further, similar to claim 11, Appellants note claim 12 requires a portion of the first cryptosync to be the second cryptosync, not merely a part of the second cryptosync. Accordingly, Appellants respectfully submit the broad, general discussion of a certificate being derived from a root certificate provided in paragraph [0145] of Malcolm is clearly insufficient to teach the specific requirement that a first cryptosync be derived **as the second cryptosync**.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 12 as is required to support a rejection under §103.

D. THE EXAMINER'S ANSWER DOES NOT ACCOUNT FOR THE FAILURE TO ESTABLISH PRIMA FACIE CASE OF OBVIOUSNESS WITH RESPECT TO EITHER OF CLAIMS 2 AND 3.

Claim 2

Appellants presented arguments in the Appeal Brief explaining why the combination of Meandzija, Malcolm and Burch fails to render the limitations of claim 2 obvious.⁹ In response, the Examiner's Answer asserts that Burch is being used to show that it is well known in the art to use digital certificates to encrypt messages, not to teach a second cryptosync or a digital certificate.¹⁰

Appellants note paragraphs [0004] and [0023] discuss the use of public key certificates for encryption. However, Appellants respectfully submit, even if, for the sake of argument, paragraphs [0004] and [0023] of Burch can be properly interpreted as teaching the use of a public key **certificate**, itself, to encrypt a message, as opposed to the well-known practice of using the digitally signed **public key** within the certificate to encrypt the message, *which Appellants do not admit*, Appellants respectfully submit the Examiner's Answer has provided no support for the assertion that the digital certificates of Meandzija of Malcolm are capable of being used to

⁹ Appeal Brief at p. 28, l. 12 – p. 30, l. 7.

¹⁰ Examiner's Answer at p. 18, l. 8 – p. 19, l. 4.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

encrypt messages. Specifically, Malcolm discusses including public keys in digital certificates and encrypting messages using the public keys¹¹. Malcolm does not appear to teach encrypting messages using digital certificates, themselves. Neither does Meandzija. Accordingly, the systems of Malcolm and Meandzija would have to be modified to meet the limitations of claim 2. However, the Examiner has provided no arguments supporting the position that it would be obvious to modify the systems of Meandzija and Malcolm such that the digital certificates of Meandzija and Malcolm, themselves, are used to encrypt messages.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 2 as is required to support a rejection under §103.

Claim 3

Claim 3 recites “wherein the second cryptosync is used for verifying message integrity by at least one of the two devices”. In responding to the arguments in the Appeal Brief regarding claim 3, the Examiner's Answer uses the same rationale used to reject claim 4 discussed above in section C of the instant Reply Brief. Accordingly, for the same reasons discussed above with respect to claim 4, Appellants respectfully submit the Office Action does not identify how any of the applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 3 as is required to support a rejection under §103.

¹¹ Malcolm at para. [0145] – [0147].

E. THE EXAMINER'S ANSWER DOES NOT ACCOUNT FOR THE FAILURE TO ESTABLISH PRIMA FACIE CASE OF OBVIOUSNESS WITH RESPECT TO CLAIM 5.

Appellants presented arguments in the Appeal Brief explaining why the combination of Meandzija, Malcolm and Somin fails to render the limitations of claim 5 obvious.¹² In response, the Examiner's Answer maintains the position that the creation of a new root certificate for a new group as taught by Somin teaches changing a second cryptosync between communication sessions.¹³ Appellants respectfully disagree.

Appellants respectfully submit the Examiner has not responded to Appellants arguments regarding the creation of a new root certificate being different from the changing of an existing root certificate. Accordingly, even if it is assumed that the root certificate of Somin constitutes a cryptosync, *which Appellants specifically refute in section A of the instant Reply Brief*, Somin still fails to teach a cryptosync that changes between communications sessions as claim 5 recites.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 5 as is required to support a rejection under §103.

¹² Appeal Brief at p. 31, l. 12 – p. 33, l. 8.

¹³ Examiner's Answer at p. 18, l. 8 – p. 19, l. 4.

F. THE EXAMINER'S ANSWER DOES NOT ACCOUNT FOR THE FAILURE TO ESTABLISH A PRIMA FACIE CASE OF OBVIOUSNESS WITH RESPECT TO CLAIMS 8-10 AND 13-23.

Claim 8

Appellants presented arguments in the Appeal Brief explaining why the combination of Meandzija, Malcolm and Rezaifar presented in the Office Action failed to render the limitations of claim 8 obvious.¹⁴ Specifically, Appellants argued that the Examiner did not explain what in Rezaifar was being interpreted as corresponding to the recited second cryptosync.

In response, the Examiner's Answer points to the same section of Rezaifar identified in the Office Action, column 4, lines 46-62.¹⁵ However, the Examiner's Answer still fails to identify where Rezaifar teaches the second cryptosync recited by claim 8.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 5 as is required to support a rejection under §103.

Claims 9, 10 and 13

Claim 9 recites "wherein the fixed bit sequence is a string of 0s". In the Appeal Brief, Appellants noted that with respect to this limitation, the Office Action referenced an EID value discussed in column 9, lines 11-22 of Rezaifar. Appellants further noted

¹⁴ Appeal Brief at p. 34, l. 4 – p. 35, l. 6.

¹⁵ Examiner's Answer at p. 20, l. 1 – 6.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

that the EID bit 807 discussed in the portion of Rezaifar referenced by the Office Action is a single bit, not a string of 0s; and that the EID bit 807 is included in a frame 800 which is not taught by Rezaifar as being a cryptosync as claim 9 requires.¹⁶

In response, on page 21 of the Examiner's Answer it is asserted that the limitation regarding the string of 0s recited in claim 9 "is not a positive step and still a step the system would be capable of doing without needing to add a positive step".¹⁷ Appellants respectfully submit the meaning of the statement quoted above is unclear. Specifically, it appears the Examiner's Answer is asserting that the limitation of claim 9 regarding the string of 0s suffers from some deficiency which permits the limitation to be ignored when considering the patentability of claim 9. However, the Examiner's Answer cites no basis in law for this assertion. Accordingly, Appellants respectfully submit the Examiner's Answer must establish that all the limitations of claim 9 are taught or otherwise rendered obvious by the cited art. This has not been done with respect to the limitation regarding the string of 0s. For at least this reason, Appellants respectfully submit a prima facie case of obviousness has not been established with respect to claim 9.

Further, Appellants note it appears Appellants' arguments regarding the frame 800, in which the EID bit 807 cited by the Examiner is included, not being a cryptosync were not addressed in the Examiner's Answer. For at least this additional reason, Appellants respectfully submit a prima facie case of obviousness has not been established with respect to claim 9.

¹⁶ Appeal Brief at p. 36, l. 10-20.

¹⁷ Examiner's Answer at p. 21, l. 10-12.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

Additionally, the Examiner's Answer maintains the position that claims 10 and 13, each of which also require a string of 0s, are obvious for the same reasons discussed above with respect to claim 9. Accordingly, for at least the same reasons discussed above with respect to claim 9, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to either of claims 10 and 13.

Claims 16 and 17

Claim 16 recites "wherein the deriving step is performed at a base station" and claim 17 recites "wherein the deriving step is performed at a mobile station". Appellants argued on page 38 the Appeal Brief¹⁸ that column 3, lines 36-45 of Rezaiifar, which were referenced by the Office Action as teaching the above-referenced limitations of claims 16 and 17, discussed subscriber units 12 and a base station 14, but did not discuss a location where any deriving is performed.

The Examiner's Answer responds to these arguments by again referencing the same section of Rezaiifar without identifying where Rezaiifar specifically teaches performing a deriving step in a mobile station or a base station.¹⁹ Appellants note a certificate authority taught by paragraph [0145] of Malcolm is also mentioned in the Examiner's Answer. However, the Examiner's Answer does not identify where any of the cited art teaches the certificate authority being located in a mobile station or a base station.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in

¹⁸ Appeal Brief at p. 38, l. 1-16.

¹⁹ Examiner's Answer at p. 21, l. 13 – p. 22, l. 2.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

combination, teach or otherwise render obvious each of the limitations of either of claims 16 and 17 as is required to support a rejection under §103.

Claim 18

Claim 18 recites "encrypting a frame of information to send from the at least one of the two devices using the first cryptosync". Appellants argued in the Appeal Brief that though column 2, lines 19-23 of Rezaifar, which were referenced by the Office Action as teaching the above-referenced limitations of claim 18, discuss encrypting traffic, the Office Action did not identify what in Rezaifar was being interpreted as teaching the recited first cryptosync.²⁰

The Examiner's Answer references the same section of Rezaifar and likewise fails to identify what is being interpreted as corresponding to the first cryptosync.²¹ For at least this reason, Appellants respectfully submit. For at least this reason, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to claim 18.

Further, for at least the reasons discussed above with reference to claim 2 in section D of the instant Reply Brief, Appellants respectfully submit the record is void of any support for the assertion that the digital certificates of Meandzija *themselves*, which the Examiner's Answer references as teaching the recited first cryptosyncs, and not the public keys within the digital certificates, are capable of being used to encrypt a message as is required of the first cryptosync recited in claim 18.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in

²⁰ Appeal Brief at p. 38, l. 19 – p. 39, l. 7.

²¹ Examiner's Answer at p. 22, l. 3-13.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

combination, teach or otherwise render obvious each of the limitations of claim 18 as is required to support a rejection under §103.

Claims 20 and 23

In the Appeal Brief, Appellants argued that the Office Action did not state how the teachings of Meandzija, Malcolm and Rezaifar were being modified or combined to teach incrementing a first cryptosync value after an encrypting step as claim 20 recites, or incrementing a first cryptosync value after a decrypting step as claim 23 recites.²²

In response, page 22, lines 14-19 of the Examiner's Answer states that Rezaifar clearly teaches the above-referenced limitations. Appellants respectfully disagree. Specifically, the Examiner's Answer asserts that the first cryptosync is taught by a session certificate. However, the Examiner's Answer cites nothing in any of the applied art teaching incrementing a session certificate. Further, neither the Office Action nor the Examiner's Answer explain how one would combine the teachings of Rezaifar with those of Meandzija and Malcolm such that a session certificate is incremented after an encryption step or a decryption step as claims 20 and 23 require of the recited first cryptosync. Further, still, neither the Examiner's Answer nor the Office Action provides a reasoning having a rational underpinning supporting the legal conclusion that it would be obvious to modify the session certificate of Meandzija such that it can be incremented as claims 20 and 23 require of the recited first cryptosync.

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner's Answer has established that any of the applied art, alone or in

²² Appeal Brief at p. 39, l. 9-22.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

combination, teach or otherwise render obvious each of the limitations of either of claims 20 and 23 as is required to support a rejection under §103.

Claim 21

Claim 21 recites “decrypting a frame of information received at the at least one of the two devices using the first cryptosync”. On page 40 of the Appeal Brief at lines 2-18, Appellants argued that the portion of Rezaifar referenced by the Office Action as teaching the above-referenced limitations of claim 21, column 5, lines 56-67, included no discussion of cryptosyncs. Further, Appellants argued that the Office Action did not explain how Meandzija, Malcolm and Rezaifar would be combined to teach the limitations of claim 21.

The Examiner’s Answer only references the same portion of Rezaifar referenced by the Office Action, and does not address any of the arguments above.²³

Accordingly, Appellants respectfully submit neither the Office Action nor the Examiner’s Answer has established that any of the applied art, alone or in combination, teach or otherwise render obvious each of the limitations of claim 21 is required to support a rejection under §103.

²³ Examiner’s Answer at p. 23, l. 1-5.

G. THE EXAMINER'S ANSWER DOES NOT ACCOUNT FOR THE FAILURE TO ESTABLISH PRIMA FACIE CASE OF OBVIOUSNESS WITH RESPECT TO CLAIM 24.

Claim 24 recites “deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions”.

In responding to the arguments in the Appeal Brief regarding claim 24, the Examiner's Answer uses the same rationale used to reject claim 1 discussed above in sections A and B of the instant Reply Brief. Accordingly, for the same reasons discussed above with respect to claim 1, Appellants respectfully submit the Office Action does not identify how any of the applied art, alone or in combination, teaches or otherwise renders obvious each of the limitations of claim 24 as is required to support a rejection under §103.

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 41.41

Atty. Dkt. No. 29250-002013/US

U.S. Appl. No. 10/786,454

IV. CONCLUSION

For at least the reasons above, a *prima facie* case of obviousness cannot be established with regard to claims 1-24. Accordingly, Appellants respectfully request the Board to reverse the Examiner's rejection.

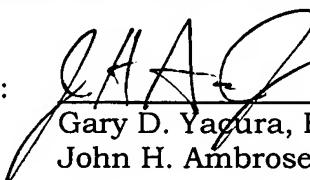
If the USPTO believes that personal communication will further the prosecution of this application, the Office is invited to contact John H. Ambrose Jr., Reg. No. 64,371, at the telephone number below.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By:



Gary D. Yacura, Reg. No. 35,416
John H. Ambrose, Jr., Reg. No. 64,371

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

GDY/JHA:eaf